BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :2**
Nom, prénom : TIZI Romain	**N° candidat :01945651796**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 06/05/2024

Organisation support de la réalisation professionnelle

La Russie, en tant que pays essentiel pour le développement mondial, a dû relever le défi de la transition vers la numérisation et l'informatisation, même dans ses plus grandes villes comme Moscou. Dans ce contexte, la sécurité et l'authentification des utilisateurs sont devenues des enjeux primordiaux pour garantir l'intégrité et la fiabilité des services offerts.

L'implémentation de solutions d'authentification robustes et sécurisées est devenue une priorité pour s'assurer que seuls les utilisateurs autorisés puissent accéder aux différents services.

Intitulé de la réalisation professionnelle

Authentification et gestion de droits

Période de réalisation : 2022/2024 **Lieu :** METZ UFA Rober Schuman

Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau
☒ Installer, tester et déployer une solution d'infrastructure réseau
☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Objectifs et résultats attendus :
Mettre en place une infrastructure d'authentification centralisée et sécurisée basée sur Active Directory
Intégrer le pare-feu Stormshield avec l'annuaire AD pour appliquer des règles d'accès en fonction des profils utilisateurs
Interfacer GLPI avec Active Directory pour synchroniser les comptes utilisateurs et gérer les habilitations
Implémenter la solution LAPS (Local Administrator Password Solution) pour sécuriser les mots de passe des comptes administrateurs locaux
Assurer une traçabilité des accès et une meilleure maîtrise des droits d'accès
Améliorer la sécurité globale du système d'information et faciliter la gestion des utilisateurs

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Les ressources utilisées sont :

- Deux serveurs Active Directory
- Un Stormshield
- Un serveur PRTG
- Serveur GLPI
- Serveur de fichiers

Modalités d'accès aux productions[3] et à leur documentation[4]

- La Procédure d'installation réalisée lors des differentes mises en place dans le contexte.
- https://romaintizi.ovh qui est l'acces au porfolio du candidat.
- Les différents accès : login : Administrateur mpd :Azerty123!
  login : prtgadmin mdp : Azerty123!

---

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

TIZI
Romain

L'Authentification

Objectif de la démarche :

L'objectif principal de cette démarche est de mettre en place une solution d'authentification efficace permettant de sécuriser l'accès aux ressources informatiques de l'organisation. Cela garantira l'intégrité des données et des systèmes, tout en facilitant la gestion des habilitations des utilisateurs.

Compétences visées :

Les principales compétences mobilisées dans cette activité sont :

2.1.3 - Élaboration d'un dossier de choix d'une solution d'infrastructure et rédaction des spécifications techniques
2.1.5 - Choix des éléments nécessaires pour assurer la qualité et la disponibilité d'un service
2.2.2 - Installation et configuration des éléments nécessaires pour assurer la continuité des services
2.2.5 - Test d'intégration et d'acceptation d'une solution d'infrastructure
2.3.1 - Administration sur site et à distance des éléments d'une infrastructure
2.3.4 - Identification, qualification, évaluation et réaction face à un incident ou à un problème
2.3.5 - Évaluation, maintien et amélioration de la qualité d'un service

Définitions et normes du domaine :

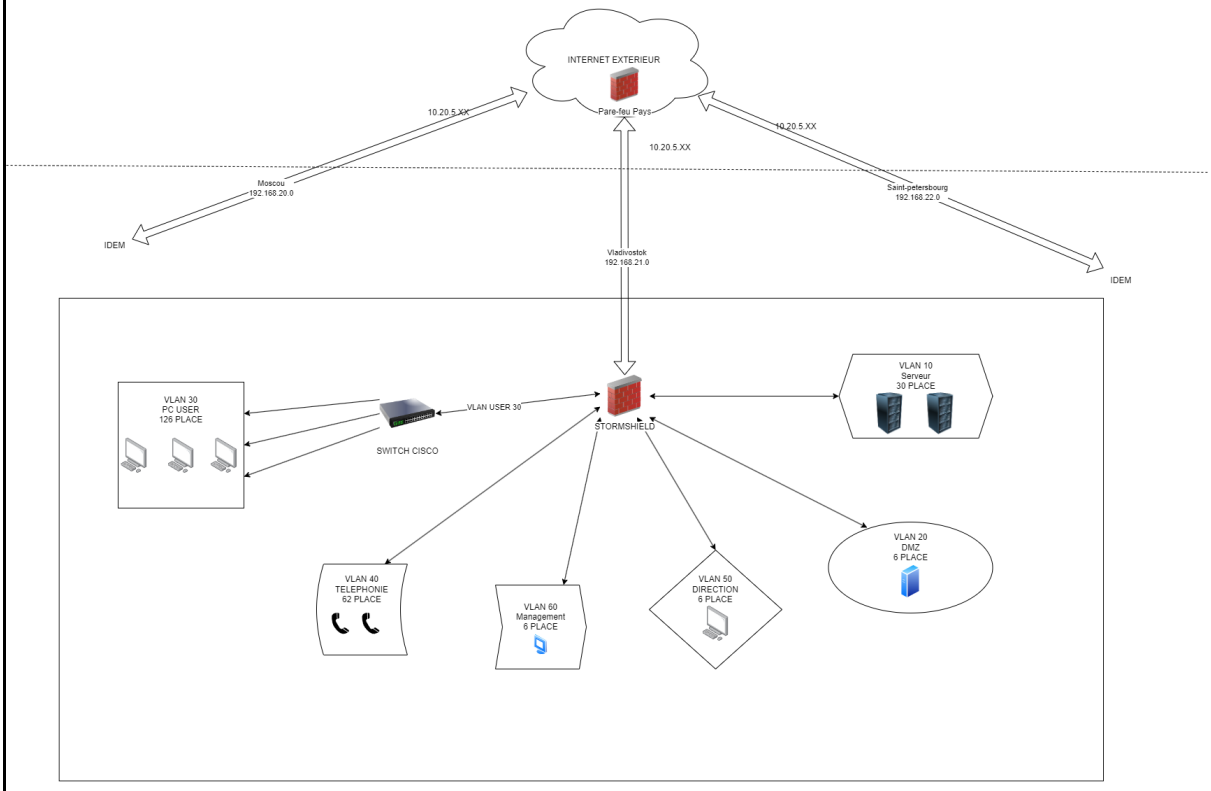
Les principaux éléments de l'authentification informatique sont :

- L'annuaire LDAP (Lightweight Directory Access Protocol) ou Active Directory (AD) : Système centralisé de gestion des comptes utilisateurs, des groupes et des droits d'accès.
- Le protocole d'authentification RADIUS (Remote Authentication Dial-In User Service) : Permet d'authentifier les utilisateurs de manière sécurisée et de leur attribuer les droits correspondants.
- L'outil GLPI (Gestion Libre de Parc Informatique) : Logiciel de gestion du parc informatique, notamment pour la gestion des utilisateurs et de leurs habilitations. GLPI peut s'interfacer avec l'annuaire Active Directory pour synchroniser les comptes utilisateurs.
- Le pare-feu Stormshield Network : Intégré avec l'annuaire LDAP, il permet d'appliquer des règles d'accès et de filtrage en fonction des groupes et des profils utilisateurs.
- LAPS (Local Administrator Password Solution) : Outil permettant de gérer de manière sécurisée les mots de passe des comptes d'administration locaux sur les postes de travail.

Contexte :

Le contexte est celui de la ville de MOSCOU en Russie, où il est crucial de sécuriser l'accès aux ressources informatiques cruciales (serveurs de fichiers, de messagerie, applications métiers, etc.). Une authentification centralisée et sécurisée est nécessaire pour garantir la confidentialité et l'intégrité des données.

Schémas et maquettes de l'infrastructure :



Plan d'adressage :

		Nom	Adresse Reseau	Commentaires	masque	broadcast	Hotes
	Vlan	SERVEUR			/27	.31	30
Serveur	10	Sauvegarde et supervison	192.168.20.3	VEEM			
	10	Fichiers	192.168.20.5	Fichiers partager			
	10	RDS	192.168.20.4	Services à distance			
	10	AD/DNS	192.168.20.1	Active Directory			
	10	DHCP	192.168.20.2	Attribution IP			
	10	AD 2	192.168.20.6	PRTG			
	10	Gestion de Parc	192.168.20.7	Glpi			
	10	Impression	192.168.20.8	Imprimante			
	10	UTM	192.168.20.9	Pare-feu			
	10	WSUS	192.168.20.10	Remplacer par log			
	10	PRTG / VEAAM	192.168.20.11				
	10	Messagerie	192.168.20.12	Mail			
	10	Téléphonie	192.168.20.13	Téléphone			
	10	IPS	192.168.20.14	Preventions intrusions			
	10	CA	192,168,20,15	Certificat et CLE			
DMZ	Vlan	WEB/DMZ			/29	.39	4
	20	WEB apach	192.168.20.33				
		web 2	192.168.20.34				
User	Vlan	Utilisateur			/25	.255	126
	30	pc 1-126	192.168.20.129-254				
Téléphonie	Vlan	Téléphonie			/26	.127	60
	40		192.168.20.64-124				
Direction	Vlan	Direction			/29	.47	6
	50		192.168.20.41-47				
Managment	Vlan	Managment			/29	.55	4
	60		192.168.20.49-53				
Accès a internet	pas de vlan	STORMSHEILD	192,168,20,9/27&		/27		
WAN		CISCO	172,15,XX,1	ou 192,168,2X,129			
		sortie storm --> cisco	172.15.22.55/24				
		Impression	192.168.20.9	Imprimante			

Connexion Stormshield avec LDAP :

Résultats et conclusion :

Les résultats attendus de cette solution d'authentification sont :
Une gestion centralisée et sécurisée des comptes utilisateurs et de leurs habilitations
Une traçabilité des accès et une meilleure maîtrise des droits
Une simplification de la gestion des mots de passe administrateurs locaux
Cela permettra d'améliorer la sécurité globale du système d'information tout en facilitant la gestion des utilisateurs et de leurs accès.

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)